Information Security Framework

State of Indiana Information Resources Policy and Practices
Indiana Office of Technology
Version 2.0

Information Security Framework Table of Contents

Introduction

The Information Security Framework establishes security policy and practices for Indiana state government. Policies provide general, overarching guidance on matters affecting security that state workforce members are expected to follow. Practices document methods and procedures as well as establish minimum compliance activities ensuring that policy objectives are met.

Security policy applies to all hardware, software, data, information, network, personal computing devices, support personnel, and users within State agencies. Going forward, these components of information technology are covered by the umbrella term of "Information Resources."

The State of Indiana Information Security Framework (ISF) has been completely reformatted and updated in this its second version. Though it still tightly follows the ISO 17799 standard, this update adopts a more common policy format and follows a more intuitive numbering scheme. For a quick overview of the organization of this document, see the high level chapter summaries below.

Overview of Chapters

Chapter 1 – Security Policy: Discusses the scope of policy, as well as roles and responsibilities.
Chapter 2 – Organizational Security: Addresses security responsibilities of the workforce, third parties, and outsourcers.
Chapter 3 – Risk Assessment and Treatment: Documents the process the state will use to identify and assess risk as well as treat the risk through controls and practices.
Chapter 4 – Asset Classification: Assures appropriate protection of state physical assets.
Chapter 5 – Human Resources Security: Addresses the considerations with state workforce members prior to employment, during employment, and after termination.
Chapter 6 – Physical and Environmental Security: Deals with the protection of physical areas and equipment from physical threats and unauthorized access.
Chapter 7 – Communications and Operations Management: Addresses the many facets of information technology operations.
Chapter 8 – System Access Controls: Tackles access restrictions for users at network, operating system, application and mobile computing levels.
Chapter 9 – System Development and Maintenance: Deals with the many aspects of application development and maintenance security concerns.
Chapter 10 – Information Security Incidents: Discusses the reporting and management requirement for security incidents.
Chapter 11 – Business Continuity: Plans for interruptions of state of Indiana business activities.
Chapter 12 – Compliance: Addresses the states compliance with laws and statutes, security policies, controls and practices as well as audit considerations.

"Just enough" security

The ideal for any environment is to have "just enough" security. It is at this point that information is secure without overspending on additional, needless layers of security. The policies contained in this document intend to encourage a balance between new or improved business opportunities and secure solutions.

Risk mitigation solutions should always consider training, process and procedural change, and other "low tech" techniques as well as sophisticated technical solutions. Historically, technical gadgets have been sold as complete solutions. In reality, they may provide only part of the solution, leaving unacceptable and perhaps unknown (to management), security vulnerabilities. Mistakenly placed trust in gadgets has left many management chains disillusioned when bitten by a security breach for which they thought they were protected.

As risks to Information Resources are identified, mitigating actions should always address root issues and not symptoms. While "just enough" security intends to put the proper emphasis on balancing security requirements with business opportunities, it should not be construed as minimizing the need for secure systems. To the contrary, any application or service exposing state Information Resources to unacceptable levels of risk should be shelved until risks can be addressed through security measures within budget constraints.

Discipline
Fortunately most state workforce members are hard working and well intended. However, when a workforce member commits a security violation, it needs to be addressed as a matter of discipline. Corrective measures will obviously vary depending on the nature of the infringement as well as the individual's work history. But it is a management responsibility to point out the error and entice proper behavior in the future to minimize continued or more flagrant mistakes. To reinforce the importance of security and assess the workforce's adherence to policy, compliance with information security policies and procedures should be considered in all workforce member performance evaluations.

Though the consequence of disciplinary action for a violation is documented directly in some policies, it is applicable to all policies and any violation.

Training
The policies contained in the Framework are easy to understand. Agencies should not hesitate to point their workforce to those of special significance to their business mission and expect them to comprehend the intent.

Policy Overlap
The policies contained in this document overlap as they follow the comprehensive construct of the ISO 177799 standard. Though there is overlap, policy themes are consistent in their intent and objectives. To have a complete understanding of the state's policy position, some issues may demand referencing more than one policy because of their granular nature.

Chapter 1 – Security Policy

1.1 – Information security policy ownership

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy identifies responsible parties for the development and maintenance of security policy while setting an objective of protecting information. Responsibilities lie with all agencies to work with the CISO to make policies complete and effective in securing the state's environment from threats.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   The Chief Information Security Officer (CISO) of the Office of Technology (IOT) shall develop information security policy and monitor for compliance. Policies and practices shall be regularly reviewed and updated as risks and mitigation methods change. The primary goal of these policies shall be to protect Information Resources commensurate with sensitivity and availability requirements. Additionally, policies shall protect the state's investment in resources which include computer resources, communications resources, and human resources.

   The CISO shall educate through appropriate means and with cooperation from agencies on policies and practices that ensure information security.

   Each state agency shall formally delegate responsibility for all information security matters and interact with the CISO as needed. Agencies shall notify the CISO of issues requiring attention through policy as well as needed modification to policy.

5. Procedures, compliance & references

   Not applicable

Chapter 1 – Security Policy

1.2 – Information security policy establishment, approval, and exceptions

Issue Date: 02/01/2006 reissued 02/27/2007
Effective Date: 02/01/2006

1. Purpose

   This policy defines the roles of those involved with security policy establishment, approval, and exceptions.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Information Security Policy Establishment
   The authority to establish information security policies is given to the State Chief Information Officer (CIO) under Indiana Code 4-13.1-2-2(a)-10. The CIO has established the Chief Information Security Officer (CISO) position and delegated authority for the development and enforcement of approved information security policies.

   Information Security Policy Approval
   Policy shall be consistent with other existing directives, laws, organizational culture, guidelines, procedures, and the State's overall mission. With these objectives in mind, IOT shall develop policy through the inclusion of State agency personnel and specialized expertise as appropriate and effective. State agency IT Directors and other appropriate audiences (dependent on content) shall review and comment on draft policy. Policy shall be periodically compared with best practices appropriately incorporating changes in technologies, personnel, and business practices. The CISO or designee shall update policies as necessary and route them back through the review process.

   Information Security Policy Exceptions
   The CISO shall consider the need for waivers or variances based upon unique legislative or business requirements to established information security policy. Requests for policy exception shall be submitted to and approved by the CISO or the CISO's designee before the waiver or exception may be implemented.

5. Procedures, compliance & references

   Not applicable

Chapter 1 – Security Policy

1.3 – Information security policy violations and enforcement

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/21/2007

1. Purpose

   This policy instructs workforce members to access only that information for which they are authorized. It also discusses disciplinary ramifications for violators. Agencies will consider the severity of the violation(s), negative ramifications, performance history, and other pertinent factors in determining the extent of discipline.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Workforce members shall only access Information Resources for which they are authorized. Accessing or attempting to access to Information Resources without authorization is prohibited and subject to disciplinary action. Agencies have the right to monitor workforce member's use of Information Resources. This includes active monitoring (e.g. – e-mail, key-logging) and historical research (e-mail history, PC Internet cache) among other measures available to agency management.

   Individuals found to be in violation of policy shall face disciplinary actions up to and including dismissal from employment. Agencies shall consider the severity of the violation(s), negative outcomes resulting from the violation, workforce member performance history, and other pertinent factors in determining the extent of discipline. Criminal prosecution is possible where the act constitutes a violation of law. A breach of contract, where applicable, may also apply.

5. Procedures, compliance & references

   - Reference Practice 8.3.1 – The Information Resources Use Agreement

Chapter 2 – Organizational Security

2.1 Information security roles and responsibilities

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy establishes that the Chief Information Security Office (CISO) and the IOT Security team are responsible for providing leadership in information security. The CISO is responsible for developing and maintaining security policy and staying abreast of security risks to personal information and working with Information Resources owners on protective measures. Agency system owners, support providers, and workforce members also have key parts in securing Information Resources.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   IOT, through the Chief Information Security Officer, shall coordinate resources to address the information security function required by the State of Indiana executive branch of state government. The Information Security organization of IOT is responsible for providing guidelines for securing information and its supporting resources. It is the responsibility of workforce members and agents of the state to communicate their security requirements for the protection of information to the Information Security organization.

   System owners shall ensure the security of their systems by coordinating and overseeing the successful execution of operating practices and policy abidance by those providing support.

   Operations support, including the State workforce and contracted resources, shall apply technologies and practices to meet the security requirements of the system.

   All workforce members shall assume responsibility for complying with the state's information security policies and shall be aware that violations of policy is grounds for disciplinary action up to and including termination.

   Independent audits of the information security program and of individual systems shall evaluate effectiveness on a regular, recurring basis.

5. Procedures, compliance & references

   Not applicable

Chapter 2 – Organizational Security

2.2 Security of third party access

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy addresses that trusted third parties may execute business on behalf of citizens in lieu of or in addition to state employees. The expectations for trusted third parties are no different than those for state employees.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Third parties shall gain access to state information assets only where there is a business need, only with approval of system owners, and only with the minimum access needed to accomplish the business objective.

   Third parties accessing the system shall be subject to the same policies and practices as are other members of the state workforce (e.g. – accepting the IRUA).

   Standard contract language shall detail the security requirements of all parties involved in an agreement with audits conducted as needed to assure compliance. State information shall be protected whether used, housed, or supported by the state workforce or third parties.

5. Procedures, compliance & references

   - Reference Practice 8.3.1 – The Information Resources Use Agreement

Chapter 2 – Organizational Security

2.3 Outsourced services contracts

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy directs agencies to include enforceable security and audit provisions in contracts and agreements.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   System owners shall assure adequate protective controls from outsourcers in the provision of services involving state Information Resources. Contractual requirements shall clearly define information protection requirements on the part of the outsourcer. These terms shall address expected protections through all aspects of operations and the lifecycles of Information Resources. Regular audits evaluate compliance with contractual terms and security requirements. Violations or failures to comply result in consequential actions determined necessary by the system owner up to and including contract termination.

   Outsourcers shall comply completely with state security policy. System owners shall provide a copy of the state's policy to the outsourcer. Requests for policy exceptions shall be submitted by the system owner, on behalf of the outsourcer, to the CISO or CISO designee.

5. Procedures, compliance & references

   Not applicable

Chapter 3 – Risk Assessment and Treatment

3.1 Assessing security risk

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy stresses the importance of conducting risk assessments on Information Resources. A formal, disciplined approach to risk identification and classification is a necessity to implement appropriate security measures.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   State agencies shall perform risk assessments on information systems and key technology assets. Mitigating risks is the shared responsibility of IOT Security and the agency owning the information asset.

   Agencies shall use a standard risk assessment methodology that is consistently repeatable and adequately considers threats to the asset. Risk assessments shall occur at regular intervals determined by threats, with the identification of new risks, or with impacting environmental changes.

   Risk assessments shall have a defined scope (enterprise, agency specific, system specific, component specific) and assign and agree to ownership of mitigation activities and compliance requirements.

5. Procedures, compliance & references

   - Practice 3.1.1 – Risk assessment for Information Resources

Chapter 3 – Risk Assessment and Treatment

3.2 Treating security risks

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy acknowledges that once risks are identified they must be treated. The clear expectation is that agencies will develop mitigation strategies and adapt their security measures appropriately throughout the lifecycle of Information Resources.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agencies shall assure the development and execution of remediation plans and the ongoing monitoring of risks to their Information Resources. Risk treatment plans must include the scope of mitigation actions and controls.

   Agencies shall develop treatment plans for risks categorized as Class 1 and Class 2 (see risk assessment practice). System and asset owners shall provide annual assessments of the risk treatment's effectiveness, evaluate the treatment's efficiency, and implement improvements.

   The asset owner shall identify the controls necessary to ensure security of the asset as well as the means for measuring their effectiveness.

   Treatment plans shall be developed with appropriate timing allowing their consideration in design stages where they can most effectively consider requirements and incorporate system controls.

5. Procedures, compliance & references

   - Reference Practice 3.1.1 – Risk assessment for Information Resources

Chapter 4 - Asset Classification and Control

4.1 Information Resources ownership

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy emphasizes that ownership of Information Resources is the key to a secure environment. Each asset must have a specific individual responsible for all aspects of its proper maintenance and protection.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   All Information Resources must have a designated owner who is responsible for the appropriate and effective use of the asset as well as its protection. Among the responsibilities are determining appropriate sensitivity classifications, criticality ratings, and access controls. Further, the owner is responsible for assuring compliance with the requirements of classifications and controls.

   In assigning information ownership when there are several possible owners, ownership assignment shall go to the individual who makes the greatest use of the information. Information owners must establish specific policies identifying the roles, functions, processes, systems and applications that may have access to the subject information assets, including the specific actions that the access privileges allow.

   Owners shall ensure workforce members and agents of the state using their resource(s) are aware of their responsibility and held accountable for its protection and preservation. Owners shall spread this awareness through appropriate communication and training.

   There shall be sufficient degree of separation of duties among workforce members and agents of the state to ensure no individual has singular, complete authority for the modification or destruction of the subject information. With the exception of computer and network operations components, IOT personnel shall not be the designated owners of any information.

5. Procedures, compliance & references

   - Reference Practice 4.2.2 - Data categorization

Chapter 4 - Asset Classification and Control

4.2 Information asset categorization

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy directs agencies to classify their information and then have the categorization drive system designs and operations support methodologies to assure availability and protective requirements are attained.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Information Resources shall be categorized regarding sensitivity and availability requirements. Risk assessments considering severity and likelihood of risks along with cost factors determine categorization. Once determined, information assets and their requirements must be kept current in an information systems inventory.

   Categorizing information shall be the responsibility of the agency that, by assignment of functional responsibilities, creates, collects or originates the information. All workforce members and agents of the state who develop information are responsible for assisting agency leadership assign the appropriate category. All workforce members and users of the information are responsible for handling it according to its assigned category.

   Categorization shall define operating requirements including but not limited to access to information, labeling and disposal rules, network and server designs, and disaster recovery planning.

5. Procedures, compliance & references

   - Practice 4.2.1 - Information Systems Inventory (ISI)
   - Practice 4.2.2 - Data categorization
   - Reference Practice 3.1.1 – Risk assessment for Information Resources

Chapter 4 - Asset Classification and Control

4.3 Public disclosure of information

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy demands that agency leadership authorize and appropriately limit the publication of information it owns.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Release of information to the general public, regardless of its categorization, shall be the responsibility of agency management owning the information. IOT or contracted hosting services are only custodians of the information with access, use, or release of agency data only given with the relevant agency's approval or as required by law enforcement.

   Workforce members, consultants, or contractors placing information in the public areas on the state's electronic infrastructure shall grant to the state the right to edit, copy, republish, and distribute such information.

5. Procedures, compliance & references

   - Reference Policy 4.4 Personal information requests, Information Security Framework

Chapter 4 - Asset Classification and Control

4.4 Personal information requests

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets guidelines for access requests. Specific emphasis is placed on IOT operations staff due to their roles and the preponderance of requests they receive to give access to information.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All workforce members with specific guidance to Office of Information Technology staff

4. Policy

   Access to agency data
   State owned information shall be used only for the purposes specifically allowed by agency management. Use of these information assets for any other reason shall not be permitted without written permission from the designated owner of the information. Unauthorized access to data by IOT Service Operations or outsourced equivalents will result in prompt disciplinary action, up to and including immediate dismissal from employment, criminal prosecution where the act constitutes a violation of law, and an action for breach of contract where applicable.

   Internal agency information requests

   a. IOT staff shall not access, use, or release agency data without the relevant agency's approval or as required by law enforcement or a court.
   b. Employees receiving requests to monitor an employee's computer use and requests for an agency's data shall only do so with direct authorization from the IOT General Counsel, CISO, or where delegated via a formalized Practice. Standard procedure routes requests through the CISO. Other authorization channels should only be used as necessary to meet customer service expectations otherwise not available. Coverage includes access to e-mails, databases, files, and other information hosted or maintained by IOT.
   c. Typical requests are made on human resources, law enforcement, or public records access grounds. Service Operations staff shall not be burdened with trying to determine appropriate authorization for the request. The IOT General Counsel and CISO will confirm authorization and then engage the appropriate Service Operations staff to properly respond to the request.
   d. Service Operations staff engaged shall keep the matter strictly confidential so that the identities of individuals are protected. Workload requirements shall be discussed with managers, but they are not entitled to know the identity of any individual subject to the request.

Public information requests

a. IOT General Counsel shall coordinate with the agency's General Counsel before responding to any public records request. IOT will never provide another agency's data in response to a public records request without the agency's approval. IOT is a custodian, not owner, of other agency's data.

IOT requests

a. IOT managers/supervisors wishing to review the files/e-mail/computer use of an IOT employee must discuss the request with the IOT General Counsel or CISO.
b. Upon approval, the General Counsel or CISO, not the manager/supervisor will engage Service Operations for assistance. Such requests shall be based on reasonable suspicion of prohibited activity and will not be a substitute for management of an employee.
c. Investigations of the General Counsel or CISO shall be conferred with the CIO.

5. Procedures, compliance & references

- Reference Practice 7.10.1 - Employee computer use monitoring, restore, review

Chapter 5 - Human Resources Security

5.1 Workforce security prior to employment

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets expectations for agencies to execute due diligence to securing their information assets through appropriate background checks of individuals. The degree of scrutiny shall vary depending on the involvement of the role with confidential or sensitive information.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   All new hires shall undergo background checks commensurate with their job duties or of those of the agencies they support. The State Personnel Department sets standards for background investigations dependent on the role of the new hire.

   Agencies shall communicate security responsibilities of the position during recruitment.

5. Procedures, compliance & references

   - SPD Policy - Background Checks for State Employment (http://intranet.spd.state.in.us/manual/bgcheck.doc)

Chapter 5 - Human Resources Security

5.2 Workforce security during employment

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy confirms to agencies that workforce members will receive training on acceptable use of state provided information assets. Training will also be provided by the agencies to address additional security requirements of their role.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   All workforce members shall receive training on acceptable use and agree to abide by the Information Resources Use agreement within three weeks of beginning employment. Failure to accept the agreement will result in a loss of access to Information Resources unless agencies grant an exception to the agreement and training.

   Agencies shall define and explain security responsibilities for the role played by the workforce member and make clear the ramifications of failing to comply. Workforce members are provided sufficient training and supporting reference materials to properly protect state owned information assets and resources.

   Workforce members shall responsibly apply this training and support to protect the state's information assets. Workforce members shall address concerns regarding an activity prior to performing that activity if appropriateness is questioned.

   Workforce members changing roles shall be appropriately subjected to additional security scrutiny and training before beginning a new role with more stringent security requirements.

5. Procedures, compliance & references

   - Reference Practice 8.3.1 – The Information Resources Use Agreement
   - Reference SPD Policy - Background Checks for State Employment (http://intranet.spd.state.in.us/manual/bgcheck.doc)

Chapter 5 - Human Resources Security

5.3 Workforce security for terminated or changed employment

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy reinforces the importance of the timely elimination of system access rights of employees leaving or changing roles in the workforce.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agencies shall assure that timely notification of terminated employees and those changing roles is provided to IOT and other technical support entities. IOT and other support providers shall promptly eliminate access capabilities of the terminated or role changing ID.

   Agencies shall confirm the return of all information assets in the possession of a terminated workforce member. An evaluation of all services used by the terminated workforce member shall determine the need for continuation (e.g. – phone, cell phone, pager, etc.).

   The immediate manager of a workforce member or agent of the state, who is leaving a position, shall review both computer-based and paper files in their possession to determine the disposition of such files.

5. Procedures, compliance & references

   - Practice 5.3.1 – Terminated ID notification

Chapter 6 - Physical and Environmental Security

6.1 Secure areas

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy instructs agencies to consider the security requirements of their business information in determining appropriate physical access limitations and protections.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state employees and contractors

4. Policy

   State agencies shall protect their physical areas consistently with the categorization of business information stored in the area regardless of format (printed, digital). Physical access to Information Resources shall be restricted to only those individuals needing access to them. Only the minimum level of access required to complete job responsibilities shall be granted to workforce members.

   Agencies shall have procedures in place minimizing third party access with visitors monitored appropriately. Keys and access badges to secured areas shall be controlled to assure only authorized personnel gain access. Workers in secure areas shall tactfully confront unrecognized visitors for authorization and thoroughly understand access rights and restrictions.

   Physical access rights shall be immediately removed for terminated staff and/or modified appropriately for staff changing roles. Agencies may grant temporary access to workforce members and/or vendors requiring additional access to Information Resources for special projects, overtime, etc., provided that the timely return to normal access is returned upon the conclusion of the project.

   Delivery loading areas for data centers shall be isolated and enable inspection of deliveries.

5. Procedures, compliance & references

   Not applicable

Chapter 6 - Physical and Environmental Security

6.2 Equipment security

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy stresses the need for agencies to have adequate physical protections, regardless of their location, for their equipment assets from purchase through disposal.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state employees and contractors

4. Policy

   Agencies shall protect their equipment, including cabling, from physical threats and unauthorized access. Equipment requiring special protection shall be isolated or employ special physical protections according to need. Equipment shall be appropriately protected from power failures and surges as well as from heat, cold and moisture.

   Equipment and software taken off-site shall be authorized by management. There shall be no differentiation in protective measures for equipment used inside or outside of the premises in cases where the information assets are the same.

   Agencies shall maintain IT equipment per manufacturer recommendations with service completed only by authorized providers.

   Destruction of obsolete and damaged equipment, including storage devices, follow DOD and IDOA Surplus guidelines.

5. Procedures, compliance & references

   Not applicable

Chapter 7 - Communications and Operations Management

7.1 Operational procedures and responsibilities

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy requires agencies to be involved and invested in the reliable, disciplined and secure management of their systems. Service providers impart technical experience and expertise but agencies must be satisfied that necessary discipline in operational support results in the meeting of expected service levels.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state employees and contractors

4. Policy

   Agencies shall ensure the correct and secure operation of information processing facilities employed by their service providers. Documented procedures shall define operating instructions and identify responsible parties and their roles.

   Change control practices shall be identified and strictly enforced. Emergency exception criteria shall be established to enable appropriate actions to prevent or in the case of a crisis. Proper communication shall be provided to all parties potentially affected by changes as well as details regarding predicted impact. Security updates to software shall be applied within pre-defined timeframes except as emergency conditions dictate.

   Service providers shall segregate duties to reduce the risk of unauthorized access, unauthorized modification, and misuse of information assets. Audit capabilities will enable the monitoring of user and administrator activities.

   All computer-resident information that is classified as sensitive must be located on computers and networks that have system access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

5. Procedures, compliance & references

   - Practice 7.1.1 – Patch management

Chapter 7 - Communications and Operations Management

7.2 Outsourced service delivery management

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets the clear expectation for agencies regarding their ownership of system information regardless of the business relationship to the application developer or host. The protection of information and SLAs of outsourced providers are to be managed aggressively and effectively.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state employees and contractors

4. Policy

   The state shall always maintain control of security aspects of services provided by third parties. Third party service providers shall be subject to documented service level agreements (SLA) that are measured and enforced.

   Third party providers shall abide by terms of contracts and agreements stipulating the processes, controls and audits to be employed to ensure the security of state information assets. Among the disciplines expected of third party providers are configuration management, capacity management, change management and disaster recovery planning.

5. Procedures, compliance & references

   - Reference Policy 2.3 Outsourced services contracts

Chapter 7 - Communications and Operations Management

7.3 System planning and acceptance

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy recognizes the importance of a structured and consistent systems development and acceptance methodology.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state employees and contractors

4. Policy

   Agencies shall structure agreements for system development in a manner assuring their completion within acceptable timeframes, consistent with cost projections, and with fulfillment of agency development architectures or industry best practices that ensure secure applications.

   Systems shall be protected from failure allowing for redundancy where required to reach service level agreements.

   System owners shall obligate their service provider to adhere to applicable programming, database, and hardware standards.

   Agencies shall not accept a system until it meets testing criteria.

   All systems shall have completed operational documentation ready prior to the system's use in a production environment. The documentation must be written so that the system may be run by persons unacquainted with it.

   Operations staff shall be trained to monitor and maintain the system.

5. Procedures, compliance & references

   - Reference Information Security Framework Chapter 9

Chapter 7 - Communications and Operations Management

7.4 Protection from malicious software

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy addresses the continual threat posed by malicious software. Malicious software has many entry points into the state's operating environment. The policy sets expectations for agencies and individual workforce members in protecting against malicious software.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state employees and contractors

4. Policy

   Agencies shall protect against malicious code by ensuring that anti-virus software is installed as part of IOT support practices on state-owned, state-operated or state-authorized information systems. IOT will set an appropriate interval for automatic updates as well as scan settings for e-mail attachments, for files and attachments from web-sites and instant messaging, and for removable media (diskettes, flash drives, CD-ROMs).

   Agencies shall ensure all software, including internally-developed application software, is free from malicious code before installation onto a computer or other system asset.

   Workforce members operating a state-owned desktop, laptop, PDA, and other applicable devices shall not distribute malicious code or disable anti-virus software. Encounters with malicious code on state-owned computing devices shall be reported to agency contacts who then notify the CISO and deploy incident management procedures as dictated by the event.

   Workforce members authorized by agency management to operate personally owned desktop, laptop, PDA, and other applicable devices for the execution of state business shall have appropriate anti-virus software installed. The purchase, technical support, and updating of this software is the responsibility of the workforce member with no state obligation. Virus infections of personally owned devices that could potentially impact state systems must be reported to appropriate management and IOT technical support for investigation.

   Agencies shall create and distribute to systems users appropriate instructional materials for malicious code security on state-owned devices as described throughout this policy.

   Agencies shall ensure that procurement processes contain assurances, including but not limited to contract terms, that any software or other deliverables are free from known malicious code.

5. Procedures, compliance & references

    - Practice 7.4.1 - Virus control

Chapter 7 - Communications and Operations Management

7.5 Data backup

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   The purpose of the Data Backup Policy is to provide for the continuity, restoration and recovery of critical data and systems. Agencies need to ensure critical data is backed up periodically and copies maintained at an off site location. Data backups are not conducted to meet agency ICPR retention requirements.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agencies

4. Policy

   All state agencies shall ensure that tape backups conform to the following best practice procedures:

   - All data, operating systems and utility files must be adequately and systematically backed up (Ensure this includes all patches, fixes and updates)
   - Records of what is backed up and to where must be maintained
   - Records of software licensing should be backed up
   - Sufficient generations of back-up data must be retained at any one time to assure data recovery and service levels for restoration are met
   - The backup media must be precisely labeled and accurate records must be maintained of backups done and to which back-up set they belong
   - Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site
   - Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they can be relied upon for use in an emergency

   Individual workstations connected to a state network shall not be backed up through a service provider as best practices dictate users store data on servers rather than locally, especially files containing personal information. In exceptional cases, responsibility for data backup on a local drive rests with the user. Where exceptions require systematic backup of workstations, the extent shall be defined, coordinated with the service provider, and tested for effectiveness.

   Agencies shall assure proper destruction of backup media when retired.

Standard backups shall not be the means of complying with records retention policy.

5. Procedures, compliance & references

   Not applicable

Chapter 7 - Communications and Operations Management

7.6 Network management

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy intends to ensure reliable and secure network services. The policy directs agencies regarding the establishment of network services and sets expectations for the providers of network services.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state employees and contractors

4. Policy

   Local area, wide area, and the campus network used by state agencies shall be supported through a means determined by the Office of Technology. Under no circumstances shall new local area networks be established or the technology of existing state networks varied, without IOT approval. Workforce members shall not connect networking gear without IOT authorization. Disciplinary actions up to and including termination of employment or contract for violators shall apply.

   Wireless networks connected to a state network must be configured and implemented by IOT.

   IOT shall maintain a documented data base for the network. This information shall be kept electronically and must be backed up regularly.

   Security patches shall be applied within established timeframes on state networking equipment.

   Network infrastructure shall be periodically scanned (e.g. quarterly or after significant changes) for known vulnerabilities. All software configurations for network equipment shall be backed up on a regular cycle (e.g. daily or weekly) with periodic off-site storage of a backup copy.

   Physical access to network devices shall be restricted to prevent unauthorized access. All physical locations housing network equipment shall be accessible only to authorized personnel both during and after normal business hours. Third party access to these facilities shall be allowed only with approval of IOT and third party adherence to documented practices while working.

   Access to management functions within network equipment shall be limited through implementation of strong authentication measures. Passwords shall change from those as

shipped from the manufacturer. Periodic password control (employees leaving, etc.) or other methods such as Radius, TACACS, or Active Directory integration shall be implemented.

Services not needed from devices shall be removed (e.g. web server, SNMP, FTP, etc.). Remaining services shall be setup with strong passwords (SNMP community strings are the equivalent of passwords and shall be changed from the vendor-provided defaults). Access control lists shall be used to limit access to services needed.

Access shall be restricted from Internet and state network locations not needed. Filters, access lists, or firewalls shall be used to limit access to the management interface and/or services available on the device.

5. Procedures, compliance & references

- Practice 7.6.1 - Wireless networks
- Practice 7.6.2 – Internet filter

Chapter 7 - Communications and Operations Management

7.7 Media handling

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy directs agencies on handling media of all types through in its use and lifecycle.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state employees and contractors

4. Policy

   Agencies shall ensure the safety of their information through appropriate media protection measures whether in use, storage, or transit. Protection schemes must consider losses from theft, unauthorized access, and environmental hazards.

   Agencies shall review media handling procedures, document storage, distribution, and disposal requirements ensuring they appropriately consider data classification. Erasure and destruction parameters shall assure disposal without data compromise.

   Agency system documentation shall specify the number of backup copies to be maintained considering importance, restoration requirements, and availability requirements.

5. Procedures, compliance & references

   Not applicable

Chapter 7 - Communications and Operations Management

7.8 Exchanging information and software

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets the integrity and security of communications in their operations.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state employees and contractors

4. Policy

   Agencies shall ensure that exchanges of information between the state, its workforce, and third parties consider relevant legislation, contractual terms, and other agreements.

   Personal information and other confidential materials shall not be included in e-mails unless as part of an agreed upon process between state agencies. Sending personal information to outside e-mail systems unless appropriately protected in transit from unauthorized disclosure and physical damage is prohibited.

   Agencies shall make certain electronic mail security prevents modification of e-mail messages and that access limitations ensure the integrity of communications. IOT shall deploy technology and expertise to reduce Spam and viruses from entry to the state's e-mail system.

   Agencies shall communicate requirements of workforce members regarding use of voice, facsimile, e-mail, and video communications.

5. Procedures, compliance & references

   Not applicable

Chapter 7 - Communications and Operations Management

7.9 Electronic commerce services

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets requirements for agencies choosing to conduct electronic commerce services.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl
05/02/2007	2.1	Update to include payment cards	C. Bradley

3. Persons, groups, systems affected

   All state employees and contractors

4. Policy

   Agencies implementing electronic commerce for receipt of payments or delivery of benefits shall be in compliance with the PCI data security standards before beginning operations and shall stay compliant or shut down the service.

   Electronic commerce transmission controls shall make certain integrity and verify authenticity while mitigating risks of introducing malicious code.

   The State of Indiana has contracted with a company specializing in Internet commerce and transactions. All systems intending to provide electronic commerce services over the Internet shall consult with the state's contracted resource to ensure consistency with the state's Internet commerce direction and with expected application safeguards.

5. Procedures, compliance & references

   PCI Standards: https://www.pcisecuritystandards.org/tech/index.htm

Chapter 7 - Communications and Operations Management

7.10 Event log monitoring

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets requirements for monitoring event logs of key Information Resources.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state employees and contractors

4. Policy

   Agencies shall monitor their applications for unauthorized information processing activities, record events, and document circumstances around anomalies.

   IOT workforce members shall monitor data communications infrastructure and all centrally supported systems, services, and applications to meet operational objectives and to maintain a secure environment. Monitoring shall include key measurements for each device supported. Authorized technicians may actively scan Information Resources to identify vulnerabilities and/or compromised hosts. Technicians shall exercise due diligence when performing any scanning activity to preserve production capabilities. Thresholds for alarms and alerts shall be configured to identify possible security breaches including intrusion prevention or detection events or violations of policy.

   IOT and authorized technicians must execute their duties respecting the privacy of others. Information discovered in the monitoring process shall not be used or disclosed for purposes other than those for which the process was approved. Exceptions include potential illegal or grossly inappropriate activities uncovered unintentionally. Such findings shall be discreetly disclosed to appropriate management for their evaluation and action.

   The state shall use video surveillance equipment in areas requiring monitoring to ensure the provision of security to both the workforce and to Information Resources.

   Any information residing on any server or workstation owned by the state, connected to the state's networks or located on state premises may be examined with appropriate justification by authorized state agency personnel or technicians acting on their behalf. This Policy includes state owned machines used at home and personal systems that are connected to the state's network (including VPN).

   Web history shall be logged for a brief period and individual activities may be researched in cases of suspected unauthorized, inappropriate, or unproductive use.

Any workforce member engaging in monitoring activities without proper authorization shall be subjected to disciplinary measures up to and including termination of employment or contract. If laws are broken, workforce members shall be subject to prosecution.

5. Procedures, compliance & references

    - Practice 7.10.1 - Employee computer use monitoring, restore, review

Chapter 8 - System Access Controls

8.1 Business requirements and access control

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets expectations for access to state information systems.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Access to Information Resources is granted by defined and documented roles. Access to Information Resources shall be consistent between workforce members in the same role. Access rights to information will be at the minimum required to successfully accomplish work responsibilities.

   Special or administrator privileges shall be granted only to workforce members needing them to complete their duties and this number shall limited to the minimum number possible without compromising service levels

5. Procedures, compliance & references

   Not applicable

Chapter 8 - System Access Controls

8.2 Workforce access management

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets expectations for workforce access to systems.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agencies shall require each workforce member to have a unique ID with Information Resources access limited only to authorized users subject to defined limitations. User access rights shall be regularly reviewed by system owners to assure optimal access to information is granted by the system.

   Workforce members shall change passwords at initial login, never share passwords, change passwords securely, and abide by the state's password management scheme.

   Agencies shall limit the number of staff with special or administrative privileges to the minimum number required to assure appropriate service levels. Workforce members shall only modify production data through an approved, controlled process.

   Auditors, information security administrators, programmers, computer operators, or system administrators shall not update production business information. Computer operations staff shall not have access to, or be permitted to, modify production business information, production programs, or the operating systems.

   Special or administrative privileges require a different ID than one used for normal business and shall only be used when performing tasks demanding the exceptional rights.

5. Procedures, compliance & references

   - Practice 8.2.1 – End user password minimums

Chapter 8 - System Access Controls

8.3 Acceptable use and user responsibilities

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets expectations for acceptable use by and responsibilities of workforce members.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   To access any information, each workforce member and agent of the state shall be required to take training on and accept the Information Resources Use Agreement. Accepting this agreement requires workforce members to agree to compliance statements indicating that they will take all necessary steps to protect the confidentiality of citizen information. It also stipulates that the use of Information Resources will be primarily for State business and that any personal use falls within agency established *de minimis* use guidelines.

   All workforce members shall accept responsibility for complying with the state's information security policies and must be aware that non-compliance with these policies is grounds for disciplinary action up to and including termination.

   Workforce members shall use their own ID and password at all times. Sharing an ID or using another's ID is strictly prohibited without a documented exception from the CISO.

   Workforce members shall have no expectation of privacy associated with the information they store in or send through these systems.

5. Procedures, compliance & references

   - Practice 8.3.1 – the Information Resources Use Agreement

Chapter 8 - System Access Controls

8.4 Network access control

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets expectations for network access.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   IOT owns responsibility for maintaining the networks used by state agencies. Information Resources connected to state of Indiana owned or operated networks shall comply with the minimum standards for security set by IOT. State agencies may develop stricter standards as dictated by their business missions. Devices that do not meet minimum standards for networked host security configurations may be disconnected.

   Access to network resources owned, operated, or paid for by the state shall be limited to authorized users and to those services required. Users shall only use external connections operated or approved by IOT. Workforce members and vendors must not make arrangements for, or actually complete the installation of, voice or data lines with any carrier or through any means without express approval from IOT management. All external connections to internal computer networks shall pass through access control point authentication prior to allowing entrance.

   Access to network resources require user authentication. Users and devices must use encrypted authentication mechanisms unless otherwise granted an exception by the CISO.

   System security requirements shall dictate segregation of networks. Network routing ensures only allowed paths to services are used. If a service is not necessary for the intended purpose or operation of a network device, that service shall not be running. Network gateways shall be equipped with needed filters.

   IOT shall inventory network equipment. Devices shall be physically located in an access controlled environment. Firmware versions shall be upgraded as soon as practical. Access to network devices shall be physically and logically limited to authorized personnel with diagnostic port access limited and audited. Changes to network device configurations shall be documented and implemented via an established change control process.

   IOT shall regularly audit network services to assure protection from security risks.

5. Procedures, compliance & references

    - Reference Practice 7.6.1 – Wireless networks

Chapter 8 - System Access Controls

8.5 Operating system access control

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/21/2006

1. Purpose

   This policy sets expectations for operating system access.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   IOT owns responsibility for maintaining servers used by state agencies. Access to servers owned, operated, or paid for by the state shall be limited to authorized users. Server access shall require user authentication with password files encrypted. Shared IDs shall be permitted only as exceptions, approved by management, and documented. Users shall be disconnected from servers at defined inactivity time-out intervals.

   IOT shall inventory servers and physically locate them in an access controlled and environmentally protected area. Server ownership shall be documented and include:

   - the server contact(s) and location, and a backup contact
   - hardware and operating system/version
   - main functions and applications

   Operating systems shall have security patches applied as soon as practical utilizing required change control procedures. User activity and security event log information shall be monitored and maintained. Operating system services unnecessary for the intended purpose service shall not be running. Administrative functions shall be performed with unique privileged IDs traceable to an individual and only when non-privileged accounts are insufficient for the necessary task. "Root" or "administrator" account use should be minimal. Access to system utilities shall be limited to authorized resources.

   IOT shall regularly audit servers to assure protection from security risks.

5. Procedures, compliance & references

   - Practice 8.5.1 – RACF administrative privileges access
   - Practice 8.5.2 – RACF RVARY

Chapter 8 - System Access Controls

8.6 Application and information access control

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets expectations for application access.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Applications shall permit only authorized users access and limit access to stored information through approved methods. Sensitive systems shall be physically and logically isolated to the degree necessary for protection.

   Applications shall have security patches applied as soon as practical utilizing required change control procedures. User activity and security event log information shall be monitored and maintained.

   Access to applications require user authentication. Users must use encrypted authentication mechanisms unless otherwise granted an exception by the CISO.

   Agencies shall regularly audit applications to assure protection from security risks.

5. Procedures, compliance & references

   Not applicable

Chapter 8 - System Access Controls

8.7 Mobile computing and teleworking

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets requirements for workforce members working at home or at off-site locations.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Workforce members authorized to work from home or off-site locations shall be subject to all state security policies and practices. Provision of equipment and connectivity shall be determined between the workforce member and state agency. Use of state provided equipment and connectivity to state networks shall be limited to authorized state workforce members. Connectivity to state networks shall be made only through IOT approved services. Home or off-site direct modem connections to a state network connected PC is prohibited.

   Storage of employee, citizen, or business personal information on home or mobile equipment (e.g. – laptop, tablet) is prohibited unless authorized by the agency. In cases where authorized, agencies shall ensure the application of any additional security measures (e.g. – encryption) required to secure personal information appropriately.

   Information stored or created on a non-state owned PC while telecommuting is the property of the state. The state may examine equipment used by its workforce regardless of ownership when circumstances merit an investigation. Workforce members shall have no expectation of privacy associated with the information they create, store, or send through these systems.

   Non-state owned devices connecting to the state network shall have appropriate operating security patches and virus protection software.

5. Procedures, compliance & references

   - Practice 8.7.1 – Personal information protection – mobile media

Chapter 9 - System Development and Maintenance

9.1 Security requirements of information systems

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets expectations that security requirements are considered in the design and development of agency applications and are considered continually through the lifecycle.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   State agencies shall identify and design security requirements in the business process of developing applications and user-developed applications. Defined security requirements shall be met through purchasing and development decisions.

   State agencies shall develop applications with secure code and develop secure code through trained staff, established standards, conducive development environments and methodologies that lead to independent third party certification as secure. Contract provisions for third-party application developments should provide enforceable and effective protection regarding application security.

   State agencies shall evaluate security history and standards of commercial software providers.

   Effective patch management programs shall be incorporated into the support and maintenance strategies for all applications.

5. Procedures, compliance & references

   Not applicable

Chapter 9 - System Development and Maintenance

9.2 Correct processing in applications

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets expectations that new applications and changes to existing applications work correctly.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   State agency applications shall implement controls and audits of their applications to prevent errors, loss, unauthorized modification, and misuse of information. System controls shall ensure data integrity and protect against corruption. Data output shall validate correct processing.

5. Procedures, compliance & references

   Not applicable

Chapter 9 - System Development and Maintenance

9.3 Cryptographic controls

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets forth requirements for using encryption technologies.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   State agencies shall apply encryption technology to assure the prevention of disclosure of electronic information to unauthorized parties. Agencies shall consider encryption technology when physical security measures are lacking or when traditional layers of security are not in place (e.g. – firewall). The ramifications of encryption on system performance shall be considered before implementation.

   State agencies deploying encryption technology shall have an encryption key management plan. This plan must ensure that data can be decrypted when access to data is necessary. This requires backup or other strategies to enable decryption to ensure data can be recovered in the event of loss or unavailability of cryptographic keys. The plan must also consider handling compromise or suspected compromise of encryption keys.

   Encrypting data at rest shall ensure information availability and compliance with public records laws, state information should be stored in a known location in unencrypted form, or if encrypted, the means to decrypt the information must be available to more than one person.

   Encrypting data in transit shall be applied where personal information faces unacceptable risk of exposure if intercepted or misrouted. A secure method shall be used to convey the decryption measure to the recipient.

   Users shall be aware of their responsibilities if given the role for maintaining control of cryptographic keys. Management of encryption keys and key management software and hardware must be under the direct supervision of a workforce member directly authorized by agency leadership.

5. Procedures, compliance & references

   Not applicable

Chapter 9 - System Development and Maintenance

9.4 Security of system files

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets requirements for securing key aspects of applications operations and testing.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agency IT project and support activities shall use appropriate controls to assure integrity and confidentiality in the eventual production system. Change control procedures protect program libraries and test data. System reviews assess the effectiveness of controls and identify improvements. Audit trails exist for all changes.

   Use of live data is prohibited for testing and all test data shall be de-personalized.

   Agencies shall restrict access to operational source program libraries. Access shall be auditable. Old versions shall be archived.

5. Procedures, compliance & references

   Not applicable

Chapter 9 - System Development and Maintenance

9.5 Development and support processes security

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy describes security requirements for systems development and support.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agencies shall strictly control project and support environments enabling the timely development of quality applications. Change control procedures to development and support environments shall require authorized, documented, and audited changes.

   Application support teams shall study operating system changes for impacts to applications and updates shall be approved by system owners.

   Agencies shall purchase applications only from reputable sources where confidence in source code quality is high. Changes to off-the-shelf software applications shall be made only in compliance with licensing terms and an overwhelming business need.

   Agencies shall manage outsourced software development to assure favorable licensing terms and certification of code quality. Continued audits to application security shall be a part of the ongoing maintenance process.

   Systems shall appropriately separate development, test, and production facilities. Development and test systems shall not use production data.

5. Procedures, compliance & references

   Not applicable

Chapter 9 - System Development and Maintenance

9.6 Technical vulnerability management

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets expectations for agencies to monitor their systems for vulnerabilities.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agencies shall ensure that application support providers proactively monitor published software vulnerabilities. Identified vulnerabilities shall be assessed for the degree of risk posed to information resources. Patches and updates addressing vulnerabilities shall be applied in a manner consistent with the level of risk. Fixes shall be evaluated and tested prior to moving into production.

5. Procedures, compliance & references

   Not applicable

Chapter 10 - Information Security Incident Management

10.1 Information security incident reporting requirements

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets expectations for reporting security incidents.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agencies shall communicate information security incidents through documenting events, identifying the scope of the incident, and notification of owners of impacted information or assets. Communications shall adhere to applicable laws and pre-defined communication procedures. Security incidents shall be reported in a timely manner. Agencies shall train staff on incident reporting requirements.

   Workforce members must report all suspected information security incidents as quickly as possible to the Information Security Organization.

5. Procedures, compliance & references

   Reference Indiana Code 4-1-11
   Reference Practices 10.1.2 – Incident handling

Chapter 10 - Information Security Incident Management

10.2 Information security incident management

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy establishes agency requirements for handling security incidents.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agencies shall report security incidents to the information security incident response team (ISERT) for their analysis and guidance in handling the incident.

   Agencies shall develop incident handling procedures that enable the effective handling of incidents by appropriate levels of technical and managerial staff. Procedures shall assure incident investigations are complete and minimize further damage.

   Agencies shall respond quickly and with organization to assure an effective response. Incidents shall be studied and preventative measures identified and implemented to inhibit recurrences.

   Agencies shall assure incident handling procedures consider the collection and handling of evidence for prosecutorial and disciplinary purposes.

5. Procedures, compliance & references

   - Practice 10.2.1 – Incident planning and management

Chapter 11 - Business Continuity

11.1 Business continuity management

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   Describe the expectations for use of State provided Information Resources.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agencies shall document plans for interruptions to business activities and protect critical business processes from the effects of major failures or disasters. Business process owners shall identify their critical processes, identify their recovery requirements, and assure recovery plans are in place.

   Agency strategies shall plan for known impacts of interruptions with measures in place to successfully restore services in defined timeframes. Plans shall identify parties and their roles and emergency procedures.

   Resumption procedures shall consider emergency and fallback plans and testing schedules. Business process owners shall assure that business continuity plans are tested and that documentation is update regularly.

5. Procedures, compliance & references

   - Reference Practice 4.2.1 - Information Systems Inventory (ISI)
   - Reference Practice 4.2.2 - Data categorization
   - Reference Practice 3.1.1 – Risk assessment for Information Resources

Chapter 12 - Compliance

12.1 Information system compliance with legal requirements

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   Describe the expectations for use of State provided Information Resources considering pertinent legislation.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agency information systems shall comply with all laws, statutes, and contractual obligations. Procedures shall be implemented to assure compliance with statutes, licensing agreements, and intellectual property rights. Procedures shall also assure the protection and retention of essential records with retention schedules following ICPR guidelines.

   Protection of personal information contained in agency systems shall meet levels required by legislation.

   Agencies shall assure Information Resources are used for authorized business purposes only.

   Evidence gathering shall conform to rules of evidence to assure admissibility and Indiana State Personnel guidelines for disciplinary purposes.

5. Procedures, compliance & references

   Not applicable

Chapter 12 - Compliance

12.2 Auditing information systems

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy instructs agencies to conduct regular security audits on their information systems.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agency information systems shall be subjected to security reviews ensuring compliance with controls and practices. System reviews shall address identified shortcomings through action plans.

5. Procedures, compliance & references

   Not applicable

Chapter 12 - Compliance

12.3 Requirements of security audits

Issue Date: 02/01/2006 reissued 02/21/2007
Effective Date: 02/01/2006

1. Purpose

   This policy sets forth requirements for conducting required information system audits.

2. Revision history

Revision Date	Revision Number	Change Made	Reviser
02/21/2007	2.0	Established in standard format	T. Stahl

3. Persons, groups, systems affected

   All state agency employees and contractors

4. Policy

   Agency information system audits shall safeguard information and productivity while being conducted. Use of audit tools will be approved by impacted support organizations and used only for authorized audits. System audit tools shall be stored appropriately to prevent misuse or compromise. Access to the tools is controlled.

   Information systems owners and application owners shall agree on system audit scope, timing, and the resolution of discovered vulnerabilities.

   Security reviews are conducted only with authorization and qualified personnel performing security tests.

5. Procedures, compliance & references

   Not applicable

Glossary

Information Resources – all hardware, software, data, information, network, personal computing devices, support personnel, and users within State agencies

CIO – the State of Indiana's Chief Information Officer

CISO – the State of Indiana's Chief Information Security Officer